

UNITED STATES DISTRICT COURT

for the
Southern District of Ohio

2020 FEB 11 PM 1:29

U.S. DISTRICT COURT
SOUTHERN DISTRICT OF OHIO
COLUMBUS

In the Matter of the Search of
(Briefly describe the property to be searched
or identify the person by name and address)
Information associated with
BEUGLING@GMAIL.COM that is stored at the
premises controlled by GOOGLE

Case No. 20mj 95

APPLICATION FOR A SEARCH WARRANT

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property (identify the person or describe the property to be searched and give its location):

See Attachment A, which is attached hereto and incorporated herein by reference

located in the Northern District of California, there is now concealed (identify the person or describe the property to be seized):

See Attachment B, which is attached hereto and incorporated herein by reference

The basis for the search under Fed. R. Crim. P. 41(c) is (check one or more):

- ☒ evidence of a crime;
☒ contraband, fruits of crime, or other items illegally possessed;
☒ property designed for use, intended for use, or used in committing a crime;
☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
21 U.S.C. §§ 841	Possess with intent to distribute a controlled substance

The application is based on these facts:

SEE AFFIDAVIT ATTACHED HERETO AND INCORPORATED BY REFERENCE HEREIN

- ☒ Continued on the attached sheet.
☐ Delayed notice _____ days (give exact ending date if more than 30 days: _____) is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Sworn to before me and signed in my presence.

Date: Feb. 11, 2020

City and state: Columbus, OH

Applicant's signature

David Barrick, DEA Task Force Officer

Printed name and title

Judge's signature

Kimberly A. Jolson, United States Magistrate Judge

Printed name and title

ATTACHMENT A

Property to Be Searched

This warrant applies to information associated with BEUGLING@GMAIL.COM that is stored at premises owned, maintained, controlled, or operated by GOOGLE, a company headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043, and preserved under GOOGLE Reference Number 3480864.

ATTACHMENT B

Particular Things to be Seized

I. Information to be disclosed by GOOGLE (the “Provider”)

To the extent that the information described in Attachment A is within the possession, custody, or control of the Provider, regardless of whether such information is stored, held or maintained inside or outside of the United States, and including any emails, records, files, logs, or information that has been deleted but is still available to the Provider, or has been preserved pursuant to a request made under 18 U.S.C. § 2703(f) on February 11, 2020, the Provider is required to disclose the following information to the government for each account or identifier listed in Attachment A, preserved under GOOGLE Reference Number 3480864:

- a. The contents of all emails associated with the account, including stored or preserved copies of emails sent to and from the account, draft emails, the source and destination addresses associated with each email, the date and time at which each email was sent, and the size and length of each email;
- b. All records or other information regarding the identification of the account, to include full name, physical address, telephone numbers and other identifiers, records of session times and durations, the date on which the account was created, the length of service, the IP address used to register the account, log-in IP addresses associated with session times and dates, account status, alternative email addresses provided during registration, methods of connecting, log files, and means and source of payment (including any credit or bank account number);
- c. The types of service utilized;
- d. All records or other information stored at any time by an individual using the account, including address books, contact and buddy lists, calendar data, pictures, and files;

e. All records pertaining to communications between the Provider and any person regarding the account, including contacts with support services and records of actions taken; and

f. For all information required to be disclosed pursuant to this warrant, the physical location or locations where the information is stored.

The Provider is hereby requested to disclose the above information to the government within 14 days of the issuance of this warrant.

II. Information to be seized by the government

All information described above in Section I that constitutes fruits, contraband, evidence, and/or instrumentalities of violations of 21 U.S.C. §§ 959, those violations involving darknet moniker TRIPWITHSCIENCE and occurring **January 1, 2017 to present**, including, for each account or identifier listed on Attachment A, preserved under GOOGLE Reference Number 3480864 information pertaining to the following matters:

- (a) The acquisition, sale and/or transport of illegal narcotics, communications between the user(s) of BEUGLING@GMAIL.COM and co-conspirators in committing the above-referenced violations, communications by or with the user(s) of BEUGLING@GMAIL.COM regarding preparatory steps in furtherance of the scheme and other evidence of the participation of the user(s) of BEUGLING@GMAIL.COM in the above-referenced violations.
- (b) Evidence indicating how and when the email account was accessed or used, to determine the geographic and chronological context of account access, use, and events relating to the crime under investigation and to the email account owner;
- (c) Evidence indicating the email account owner's state of mind as it relates to the crime under investigation;
- (d) The identity of the person(s) who created or used the user ID, including records that help reveal the whereabouts of such person(s).
- (e) The identity of the person(s) who communicated with the BEUGLING@GMAIL.COM about matters relating to 21 U.S.C. §§ 959, including records that help reveal their whereabouts.

IN THE UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF OHIO

IN THE MATTER OF THE SEARCH OF
INFORMATION ASSOCIATED WITH
BEUGLING@GMAIL.COM THAT IS
STORED AT PREMISES CONTROLLED
BY GOOGLE

Case No.

Filed Under Seal

AFFIDAVIT IN SUPPORT OF
AN APPLICATION FOR A SEARCH WARRANT

I, Task Force Officer David Barrick, being first duly sworn, hereby depose and state as follows:

INTRODUCTION AND AGENT BACKGROUND

1. I make this affidavit in support of an application for a search warrant for information associated with a certain account that is stored at premises controlled by GOOGLE, an email provider headquartered at 1600 Amphitheatre Parkway, Mountain View, California, 94043. The information to be searched is described in the following paragraphs and in Attachment A. This affidavit is made in support of an application for a search warrant under 18 U.S.C. §§ 2703(a), 2703(b)(1)(A) and 2703(c)(1)(A) to require GOOGLE to disclose to the government copies of the information (including the content of communications) further described in Section I of Attachment B. Upon receipt of the information described in Section I of Attachment B, government-authorized persons will review that information to locate the items described in Section II of Attachment B.
2. I am currently employed as a Sergeant by the Franklin County Sheriff's Office, and I have concurrently been serving as a Task Force Officer with the Drug Enforcement Administration (hereinafter referred to as "DEA") since May of 2019. Being duly appointed according to law and acting as such, I am an investigative or law enforcement officer within

the meaning of 18 U.S.C. § 2510(7), that is, an officer of the United States who is empowered by law to conduct investigations and to make arrests for offenses enumerated in 18 U.S.C. § 2516. In those capacities, I have participated in investigations involving the debriefing of illegal narcotics traffickers, review of electronic information obtained pursuant to search warrants issued to electronic communications providers, review of telephone records and GPS data, review of money transfer records, surveillance, analysis of pen register information, review of electronically stored communications, and various other investigative techniques. As a result of my training and experience, I am familiar with the techniques and methods of operation used by individuals involved in criminal activity to conceal their activities from detection by law enforcement authorities, to communicate with co-conspirators known and unknown, and to arrange for the transport of contraband, including narcotics.

3. The facts in this affidavit come from my personal observations, my training and experience, as well as my review of documents and information obtained from other law enforcement personnel and witnesses. Because the purpose of this affidavit is limited to demonstrating probable cause for the requested warrant, it does not set forth all of my knowledge about this matter. In addition, when I rely on statements made by others, such statements are set forth only in part and in sum and substance unless otherwise indicated.

4. Based on my training and experience and the facts as set forth in this affidavit, there is probable cause to believe that violations of 21 U.S.C. §§ 841 have been committed by the user of GOOGLE email account BEUGLING@GMAIL.COM, and his/her co-conspirators. There is also probable cause to search the information described in Attachment A for evidence, instrumentalities, contraband, and/or fruits of these crimes further described in Attachment B.

JURISDICTION

5. This Court has jurisdiction to issue the requested warrant because it is “a court of competent jurisdiction” as defined by 18 U.S.C. § 2711. 18 U.S.C. §§ 2703(a), (b)(1)(A), & (c)(1)(A). Specifically, the Court is “a district court of the United States . . . that has jurisdiction over the offense being investigated.” 18 U.S.C. § 2711(3)(A)(i).

PROBABLE CAUSE

6. In October of 2019, members of the Drug Enforcement Administration (DEA) Columbus District Office (CDO) initiated an investigation into the illegal narcotics trafficking activities of darknet moniker TRIPWITHSCIENCE. Based upon investigative efforts to date, as well as information obtained from preceding linked investigations, law enforcement has learned that darknet moniker TRIPWITHSCIENCE, is situated at the head of a drug trafficking organization (DTO). TRIPWITHSCIENCE is responsible for the advertisement, usage, and distribution of 4-acetoxy-N,N-dimethyltryptamine (4-AcO-DMT), an analog of liquid Psilocyn (aka: liquid mushrooms), a schedule I drug under the Controlled Substances Act when sold for human consumption. Darknet vendors, such as TRIPWITHSCIENCE, process orders for drugs via the darknet and use parcel delivery services, such as FedEx, United Parcel Service (UPS), and the United States Postal Service (USPS), to deliver the orders to their customers. Illegal narcotic shipments have been located throughout the United States, other foreign countries, and portions of the illegal narcotic shipments have arrived in the Southern District of Ohio for distribution.

7. October 2019, the Agents from the DEA CDO conducted a search warrant on the residence of a Source of Information, herein referred to as SOI. During the search

warrant, the SOI signed over his/her darknet account to investigators. Investigators checked the account's recent orders and saw that the SOI purchased "liquid mushrooms" and was awaiting delivery from vendor TRIPWITHSCIENCE. Prior to its delivery to the SOI, United States Postal Inspection Service (USPIS) Postal Inspector Mohamed Sabrah was able to intercept said parcel and obtained a search warrant to open the parcel. The parcel was found to contain suspected liquid Psilocin.

8. On October 17, an interview was conducted with the SOI. During the interview, the SOI admitted he/she had four unopened parcels containing drugs at his/her residence. The SOI admitted he/she purchased the parcels from TRIPWITHSCIENCE via the darknet. At the conclusion of the interview, the SOI turned over the parcels to Inspector Sabrah and gave consent for Inspector Sabrah to seize and open the parcels. The four parcels were found to contain suspected liquid Psilocin.

9. On December 11, an investigative search was conducted on the darknet Empire Market for vendor TRIPWITHSCIENCE advertising psychedelics for sale, specifically unlimited quantities of "Liquid Mushrooms (Pure Psilocybin Extract)". According to postings from the vendor page of TRIPWITHSCIENCE, advertisements for "Liquid Mushrooms" are being sold for human consumption. This search revealed TRIPWITHSCIENCE was active on Empire Market and had 2,555 transactions on Empire Market since December 3, 2018.

10. TRIPWITHSCIENCE stated in their profile that he/she was previously active on additional darknet markets. An investigative search on TRIPWITHSCIENCE into other darknet markets revealed he/she had completed an additional 8,000 total market transactions.

11. Database records of a seized darknet market located bitcoin wallet addresses used by the moniker TRIPWITHSCIENCE. Using open source investigative tools,

investigators were able to determine a unique crypto-currency wallet address belonged to the Paxful crypto-currency exchange. Paxful was served a subpoena for the subscriber information and account history associated with the Paxful wallet address mentioned above. Paxful subpoena returns revealed the wallet address was attributed to Paxful User 561672. User 561672 provided the email address beugling@gmail.com to Paxful. Paxful further captured a unique IP address from user 561672 during maintenance of the account. Cellco Partnership DBA Verizon Wireless was served a subpoena for the subscriber information associated with the listed IP address. Cellco Partnership DBA Verizon Wireless subpoena returns revealed the user using the listed IP address was Brandon EUGLING, telephone number (708) 927-4685, with a billing address of 10505 Parkside Ave. Apt. 2F, Chicago, IL 60415-2063.

12. An investigative search substantiated EUGLING is associated with the address 10505 Parkside Ave. Apt. 2F, Chicago Ridge, IL 60415-2063, the email address beugling@gmail.com, and telephone number (708) 927-4685.

13. On December 13, Homeland Security Investigations Special Agent Justin Myers conducted a law enforcement-controlled buy of "liquid mushrooms" from the darknet Empire Market vendor TRIPWITHSCIENCE. On December 23, SA Myers received one domestic United States Postal Service mail parcel containing approximately 45 milligrams of suspected liquid psilocybin mushrooms. Lab analysis determined the suspected liquid psilocybin mushrooms to contain approximately 75.01g of 4-acetoxy-N,N-dimethyltryptamine (4-AcO-DMT).

14. On December 23, Homeland Security Investigations Special Agent Justin Myers conducted a law enforcement-controlled buy of "liquid mushrooms" from the darknet

Empire Market vendor TRIPWITHSCIENCE. On January 3, 2020, SA Myers received one domestic United States Postal Service mail parcel containing approximately 45 milligrams of suspected liquid psilocybin mushrooms. Lab analysis determined the suspected liquid psilocybin mushrooms to contain approximately 76.32g of 4-acetoxy-N,N-dimethyltryptamine (4-AcO-DMT).

15. On December 31, 2019 SA Justin Myers conducted a law enforcement-controlled buy of “liquid mushrooms” from the darknet Empire Market vendor TRIPWITHSCIENCE. On January 7, 2020, SA Myers received one domestic United States Postal Service mail parcel containing approximately 45 milligrams of suspected liquid psilocybin mushrooms. Lab analysis pending.

16. On February 11, 2020, a preservation request was served upon GOOGLE, thereby ensuring the evidence sought remains in the care and control of GOOGLE. In general, an email that is sent to a GOOGLE subscriber is stored in the subscriber’s “mail box” on GOOGLE servers until the subscriber deletes the email. If the subscriber does not delete the message, the message can remain on GOOGLE servers indefinitely. Even if the subscriber deletes the email, it may continue to be available on GOOGLE’s servers for a certain period of time.

17. On February 11, 2020, GOOGLE confirmed via responsive email the preservation of the evidence being sought, storing the responsive evidence under Reference Number 3480864.

BACKGROUND CONCERNING EMAIL

18. In my training and experience, I have learned that GOOGLE provides a variety of online services, including electronic mail (“email”) access, to the public. GOOGLE allows subscribers to obtain email accounts at the domain name gmail.com, like the email account listed in Attachment A. Subscribers obtain an account by registering with GOOGLE. During the registration process, GOOGLE asks subscribers to provide basic personal information. Therefore, the computers of GOOGLE are likely to contain stored electronic communications (including retrieved and unretrieved email for GOOGLE subscribers) and information concerning subscribers and their use of GOOGLE services, such as account access information, email transaction information, and account application information. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users.

19. In my training and experience, email providers generally ask their subscribers to provide certain personal identifying information when registering for an email account. Such information can include the subscriber’s full name, physical address, telephone numbers and other identifiers, alternative email addresses, and, for paying subscribers, means and source of payment (including any credit or bank account number). In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account’s user or users. Based on my training and my experience, I know that, even if subscribers insert false information to conceal their identity, this information often provides clues to their identity, location, or illicit activities.

20. In my training and experience, email providers typically retain certain transactional information about the creation and use of each account on their systems. This information can include the date on which the account was created, the length of service, records of log-in (*i.e.*, session) times and durations, the types of service utilized, the status of the account (including whether the account is inactive or closed), the methods used to connect to the account (such as logging into the account via the provider's website), and other log files that reflect usage of the account. In addition, email providers often have records of the Internet Protocol address ("IP address") used to register the account and the IP addresses associated with particular logins to the account. Because every device that connects to the Internet must use an IP address, IP address information can help to identify which computers or other devices were used to access the email account.

21. In my training and experience, in some cases, email account users will communicate directly with an email service provider about issues relating to the account, such as technical problems, billing inquiries, or complaints from other users. Email providers typically retain records about such communications, including records of contacts between the user and the provider's support services, as well as records of any actions taken by the provider or user as a result of the communications. In my training and experience, such information may constitute evidence of the crimes under investigation because the information can be used to identify the account's user or users.

22. This application seeks a warrant to search all responsive records and information under the control of GOOGLE, a provider subject to the jurisdiction of this court, regardless of where GOOGLE has chosen to store such information. The government intends to require the disclosure pursuant to the requested warrant of the contents of wire or electronic

communications and any records or other information pertaining to the customers or subscribers if such communication, record, or other information is within GOOGLE's possession, custody, or control, regardless of whether such communication, record, or other information is stored, held, or maintained outside the United States.¹

23. As explained herein, information stored in connection with an email account may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, the information stored in connection with an email account can indicate who has used or controlled the account. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. For example, email communications, contacts lists, and images sent (and the data associated with the foregoing, such as date and time) may indicate who used or controlled the account at a relevant time. Further, information maintained by the email provider can show how and when the account was accessed or used. For example, as described below, email providers typically log the Internet Protocol (IP) addresses from which users access the email account, along with the time and date of that access. By determining the physical location associated with the logged IP addresses, investigators can understand the chronological and geographic context of the email account access and use relating to the crime under investigation. This geographic and timeline information may tend to either inculcate or exculpate the account owner. Additionally, information stored at the user's account may further indicate the geographic location of the account user at a particular time (*e.g.*, location information integrated into an

image or video sent via email). Last, stored electronic data may provide relevant insight into the email account owner's state of mind as it relates to the offense under investigation. For example, information in the email account may indicate the owner's motive and intent to commit a crime (*e.g.*, communications relating to the crime), or consciousness of guilt (*e.g.*, deleting communications in an effort to conceal them from law enforcement).

CONCLUSION

24. Based on the forgoing, I request that the Court issue the proposed search warrant. Because the warrant will be served on GOOGLE, who will then compile the requested records at a time convenient to it, reasonable cause exists to permit the execution of the requested warrant at any time in the day or night.

Respectfully submitted,



David Barrick
Task Force Officer
Drug Enforcement Administration

Subscribed and sworn to before me on Feb. 11, 2020



Honorable Kimberly A. Jolson
UNITED STATES MAGISTRATE JUDGE

